CLAIMS

What is claimed is:

1. A method for monitoring a database, comprising:
collecting user behavior data that indicates how one or more users use the database;
processing and storing the data as historical data;
analyzing the historical data to determine behavior patterns;
receiving a new set of data that indicates how one or more users have used the database;
performing a comparison between the new set of data and the behavior pattern;
determining based on the comparison, whether the new set of data satisfies a set of criteria;
if the new set of data satisfies the set of criteria, then determining that the new set of data represents anomalous activity; and
responding to the determination by performing a targeted operation.

2. The method of claim 1, further comprising:
determining if the new set of data violates a rule based policy; and
if the new set of data violates the rule based policy, then determining that the new set of data represents anomalous activity.

3. The method of claim 2, wherein collecting user behavior data further comprises:
reading information from an audit trail or dynamic performance views of the database manager.

4. The method of claim 3, wherein collecting user behavior data further comprises collecting information at a monitoring level selected from at least one of:
information about database access for one or more selected database objects;
information about database access for one or more selected database users; and
information about database access for one or more selected database user sessions.

5. The method of claim 3, wherein collecting user behavior data further comprises:
receiving a type of information to be monitored;
determining a monitoring level from the type of information; and
activating audit options of the database manager based upon the monitoring level determined.

6. The method of claim 2, wherein analyzing the historical data to determine behavior patterns further comprises:
determining a statistical model from the historical data.

7. The method of claim 6, wherein determining a statistical model from the historical data further comprises:
determining a frequency of database access from the historical data;
determining a probability function for frequencies of database access; and
determining a cumulative probability function from the probability function.

8. The method of claim 7, wherein performing a comparison between the new set of data and the behavior pattern further comprises:

testing a hypothesis using the new set of data against the statistical model.

9. The method of claim 8, wherein testing a hypothesis using the new set of data against the statistical model further comprises:

determining a frequency of database access for the new set of data; and

determining the threshold value from a guard criteria and a probability function parameter.

10. The method of claim 9, wherein testing a hypothesis using the new set of data against the statistical model pattern further comprises:

comparing the frequency of database access for the new set of data with the threshold value.

11. The method of claim 7, wherein the historical information is about database access for one or more selected database objects and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of:

object access frequency by hour of day, object access frequency by hour of day and operating system user, object access frequency by hour of day and database user, object access frequency by hour of day and location, object access frequency by hour of day and combination of at least two of operating system user, database user and location.

12. The method of claim 7, wherein the historical information is about database access for one or more selected database users and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of:

user access frequency by hour of day, user access frequency by hour of day and operating system user, user access frequency by hour of day and database user, user access frequency by hour of day and location, user access frequency by hour of day and a combination of at least two of operating system user, database user, and location.

13. The method of claim 7, wherein the historical information is about database access for one or more selected database user sessions and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of:

number of page reads per session, access duration per session, number of page reads per unit time.

14. The method of claim 1, wherein performing a targeted operation comprises at least one of: raising an alert; sending an email; producing a report; performing a visualization.

15. A computer-readable medium carrying one or more sequences of instructions for reverting to a recovery configuration in response to device faults, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

collecting user behavior data that indicates how one or more users use the database;

processing and storing the data as historical data;

analyzing the historical data to determine behavior patterns;

receiving a new set of data that indicates how one or more users have used the database;

performing a comparison between the new set of data and the behavior pattern;

determining based on the comparison, whether the new set of data satisfies a set of criteria;

if the new set of data satisfies the set of criteria, then determining that the new set of data represents anomalous activity; and

responding to the determination by performing a targeted operation.

16. The computer-readable medium of claim 15, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

determining if the new set of data violates a rule based policy; and

if the new set of data violates the rule based policy, then determining that the new set of data represents anomalous activity.

17. The computer-readable medium of claim 16, wherein the instructions for carrying out the step of collecting user behavior data further comprise instructions for carrying out the step of:

reading information from an audit trail of the database manager.

18. The computer-readable medium of claim 17, wherein the instructions for carrying out the step of collecting user behavior data further comprise instructions for carrying out the step of collecting information at a monitoring level selected from at least one of:

information about database access for one or more selected database objects;

information about database access for one or more selected database users; and

information about database access for one or more selected database user sessions.

19. The computer-readable medium of claim 17, wherein the instructions for carrying out the step of collecting user behavior data further comprise instructions for carrying out the steps of:

receiving a type of information to be monitored;

determining a monitoring level from the type of information; and

activating audit options of the database manager based upon the monitoring level determined.

20. The computer-readable medium of claim 16, wherein the instructions for carrying out the step of analyzing the historical data to determine behavior patterns further comprise instructions for carrying out the step of:

determining a statistical model from the historical data.

21. The computer-readable medium of claim 20, wherein the instructions for carrying out the step of determining a statistical model from the historical data further comprise instructions for carrying out the step of:

determining a frequency of database access from the historical data;

determining a probability function for frequencies of database access; and

determining a cumulative probability function from the probability function.

22. The computer-readable medium of claim 21, wherein the instructions for carrying out the step of performing a comparison between the new set of data and the behavior pattern further comprise instructions for carrying out the step of:

testing a hypothesis using the new set of data against the statistical model.

23. The computer-readable medium of claim 22, wherein the instructions for carrying out the step of testing a hypothesis using the new set of data against the statistical model further comprise instructions for carrying out the steps of:

determining a frequency of database access for the new set of data; and

determining the threshold value from a guard criteria and a probability function parameter.

24. The computer-readable medium of claim 23, wherein the instructions for carrying out the step of testing a hypothesis using the new set of data against the statistical model further comprise instructions for carrying out the step of:

comparing the frequency of database access for the new set of data with the threshold value.

25. The computer-readable medium of claim 21, wherein the historical information is about database access for one or more selected database objects and wherein the instructions for carrying out the step of determining a frequency of database access from the historical data further comprise instructions for carrying out the step of determining a frequency of at least one of:

object access frequency by hour of day, object access frequency by hour of day and operating system user, object access frequency by hour of day and database user, object access frequency by hour of day and location and object access frequency by hour of day and a combination of at least two of operating system user, database user and location.

26. The computer readable medium of claim 21, wherein the historical information is about database access for one or more selected database users and wherein the instructions for carrying out the step of determining a frequency of database access from the historical data further comprise instructions for carrying out the step of determining a frequency of at least one of:

user access frequency by hour of day, user access frequency by hour of day and operating system user, user access frequency by hour of day and database

user, user access frequency by hour of day and location and user access frequency by hour of day and a combination of at least two of operating system user, database user, and location.

27. The computer readable medium of claim 21, wherein the historical information is about database access for one or more selected database user sessions and wherein the instructions for carrying out the step of determining a frequency of database access from the historical data further comprise instructions for carrying out the step of determining a frequency of at least one of:
number of page reads per session, access duration per session, number of page reads per unit time.

28. The computer readable medium of claim 15, wherein the instructions for carrying out the step of performing a targeted operation comprises comprise instructions for carrying out at least one of: raising an alert; sending an email; producing a report; performing a visualization.

29. An apparatus, comprising:
means for collecting user behavior data that indicates how one or more users use the database;
means for processing and storing the data as historical data;
means for analyzing the historical data to determine behavior patterns;
means for receiving a new set of data that indicates how one or more users have used the database;

means for performing a comparison between the new set of data and the behavior pattern;

means for determining based on the comparison, whether the new set of data satisfies a set of criteria;

means for determining that the new set of data represents anomalous activity, if the new set of data satisfies the set of criteria; and

means for responding to the determination by performing a targeted operation.

30. An apparatus, comprising:

a data collector for collecting user behavior data that indicates how one or more users use the database and processing and storing the data as historical data; and receiving a new set of data that indicates how one or more users have used the database;

a data analyzer for analyzing the historical data to determine behavior patterns; and

an anomaly detector for performing a comparison between the new set of data and the behavior pattern; determining based on the comparison, whether the new set of data satisfies a set of criteria; determining that the new set of data represents anomalous activity if the new set of data satisfies the set of criteria; and responding to the determination by performing a targeted operation.